US-PAT-NO: 6170744
DOCUMENT-IDENTIFIER: US 6170744 B1
TITLE: Self-authenticating negotiable documents
DATE-ISSUED: January 9, 2001
INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Lee; Warren S.	Jacksonville	FL	N/A	N/A
Meadow; William D.	Jacksonville	FL	N/A	N/A

US-CL-CURRENT: 235/380,235/382 ,380/55 ,902/2

ABSTRACT: A self-authenticating document is created by providing a one-way hash value in a symbol creation process, and then using a public key to decrypt data of the self-authenticating document . Raw data to be provided with the self-authenticating document is received, and an account digital signature key is retrieved and used to sign the raw data. A non-repudiation hash value from a previously-created self-authenticating document is utilized, and the raw data and the digital signature key is combined with the hash value to create a new hash value for the self-authenticating document . The hashed data is then encrypted, and any non-encrypted fields are merged in to create a full data packet. The full data packet is used to provide a self-authenticating symbol, such as a bar code label, on the self-authenticating document . The self-authenticating code is used during a document verification step to ensure that the document is genuine. The non-encrypted data within the self-authenticating code contains flags indicating which public key should be used to decrypt the encrypted data within the self-authenticating code. After decryption, a checksum is performed and compared against a checksum value stored in the decrypted portion of the self-authenticating code. If they match, and if a digital signature within the self-authenticating code is verified using an appropriate public key, the document is determined to be authentic.

14 Claims, 4 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 4

ABPL: A self-authenticating document is created by providing a one-way hash value in a symbol creation process, and then using a public key to decrypt data of the self-authenticating document . Raw data to be provided with the self-authenticating document is received, and an account digital signature key is retrieved and used to sign the raw data. A non-repudiation hash value from a previously-created self-authenticating document is utilized, and the raw data and the digital signature key is combined with the hash value to create a new hash value for the self-authenticating document . The hashed data is then encrypted, and any non-encrypted fields are merged in to create a full data packet. The full data packet is used to provide a self-authenticating symbol, such as a bar code label, on the self-authenticating document . The self-authenticating code is used during a document verification step to ensure that the document is genuine. The non-encrypted data within the self-authenticating code contains flags indicating which public key should be used to decrypt the encrypted data within the self-authenticating code. After decryption, a checksum is performed and compared against a checksum value stored in the decrypted portion of the self-authenticating code. If they match, and if a digital signature within the self-

authenticating code is verified using an appropriate public key, the document is determined to be authentic.

BSPR: U.S. Pat. No. 5,594,226, issued to Steger et al., discloses an automated check verification system in which a bar code is printed onto a check . A bar code scanner reads the information contained in the bar code, and based on that information, determines a bank code and an account code. The proper bank, traveler's check company, or money order company is then contacted automatically, to determine the account status. Based on the account status, the check will or will not be processed. This process only verifies that sufficient funds exist in the account to cover or honor the document presented, is does not indicate if the request should be honored or the funds transferred. Steger works to prevent the acceptance of bad or NSF (Non-Sufficient-Fund) checks. Steger et al. has no provision for authenticating the creator of the check as being authorized to do so, nor does Steger et al. authenticate or verify that data on the check (i.e., the amount, etc.) has or has not been modified. Summarizing, Steger et al. only addresses the availability of funds.

BSPR: U.S. Pat. No. 5,432,506, issued to Chapman, discloses a counterfeit document detection system, in which a secret program selects certain characters written or already on the document, and then transforms those characters into strings of characters to print on the document as a unique code . While Chapman's system may increase the likelihood of detecting that data on a document has been modified, it may not be able to detect all such changes, since it uses key data points spaced in sporadic locations across the face of the document as checkpoints. Alterations between these checkpoints will not be detected. Further, only a single layer of authentication/verification is performed by Chapman's system.

BSPR: The above-mentioned objects and other advantages of the invention may be achieved by a method for authenticating and validating contents of a data symbol. The method includes a step of determining if the data symbol has been encrypted, and if so, decrypting the data symbol using a public key. The method also includes a step of computing a check sum on the decrypted data symbol. The method further includes a step of comparing the computed check sum with a check sum value included in the data symbol and retrieved from the data symbol through the decrypting of the data symbol to determine if the decrypted data symbol is error free. The method still further includes a step of verifying a digital signature provided with the data symbol using a public digital signature key. If the comparison in the third step and the verification in the fourth step are successful, the data symbol is authenticated and validated. The data contained in the symbol may now be used to authenticate the contents of the human readable portions of the document .

BSPR: The above-mentioned objects and other advantages of the invention may be achieved by a system for creating a self-authenticating check . The system includes a database containing, or a methodology for managing, the data to be used in creating the self-authenticating check . The system also includes a validation unit communicatively coupled to the database/data management system and configured to receive the data and to validate whether or not the data can be used in creating the self-authenticating check . The system further includes a merge image and signature unit communicatively coupled to the validation unit and configured to merge an account physical signature, a physical signature code, public and private keys, logo's and other facial characteristics of the document with the data received from the validation unit. The system still further includes an encryption unit communicatively coupled to the merge image and signature unit and configured to encrypt the data with the account digital signature key. The system also includes a symbol creation unit communicatively coupled to the encryption unit and configured to further encrypt the data using a PPK based encryption algorithm (e.g.--RC6, ECC) and by storing it in a symbol based format. This unit also computes the one way hash value using a secure hashing function and the value of a previously created document. The merge image and signature unit merges the encrypted data output from the symbol creation unit with non-encrypted data to be used for decryption. The system also includes a printing unit communicatively coupled to the merge image and signature unit and configured to print a self authenticating symbol onto the encrypted data output by the merge image and signature unit.

DEPR: Banks that have image capable compatible check reader systems, such as NCR's Model 7780, can readily offer a fraud-proof system and method to their customer base without the added complexities of Positive Pay or ACH. According to the invention, information is encrypted at the time of document creation, using a public key/private key methodology. This information is then stored as a PDF (or similar type of file) that is printed on the document itself. FIG. 1 shows such a check, in which PDF is printed as a two-dimensional bar code 110 onto the bottom-middle portion of the check 100. The PDF can be printed in nay location on the document so long as it does not interfere with other reserved or allocated areas. The bar code 110 contains information used to authenticate the document, such as payee's name, invoice #, amount of check, hash code, public key, account #, check #, and date of check.

DEPR: In the invention, each customer has a check printing system, preferably a laser check printing system. Other types of printing systems, such as ink-jet printing systems, may be utilized instead of laser-based printers. The customers would be provided with all of the software, along with the interface to each customer's accounting system, necessary for creation and printing of self-authenticating checks according to the invention. As a result, system modification, file transfer capabilities, software upgrades and other hassles and inconveniences normally associated with Positive Pay/ACH installations are eliminated. The only requirement for potential customers is the readily available printer for printing the self-authenticating codes on the face of the documents . For example, each customer would have an MICR-capable laser printer for that purpose.

DEPR: Using a public/private key methodology, all data necessary to authenticate the document is encrypted, and then output in a process flow 525. A separate non-reputable one-way hash is computed.

DEPR: In process flow 550, the decrypt symbol portion 664 of the symbol processor 660 retrieves, from a key manager 665, the encryption keys necessary. In process flows 555 and 560, the symbol processor 660 performs the necessary decoding and validation procedures, and if verified (by the authenticate document portion 662 of the symbol processor 660), uses the data to validate the data on the face of the document (e.g., handwritten amount of check, handwritten name of payee). This includes comparisons with any MICR data encoded during the clearing house operations. A check for duplicate document submissions is also performed at this stage.

DEPR: Negotiable document fraud can be categorized into three main classifications. Document duplication, document alteration, and counterfeit documents. The invention is a closed loop system encompassing both document generation as well as the back end processing and clearing functions. The variable data is captured and encrypted during the document creation process. According to the invention when the document reaches the first point in the clearing process, the PDF is read and decrypted using the appropriate public-private key set. This point may include the bank of first deposit, a check cashing facility, or a retailer. The ability to produce valid results using a PPK encryption and/or digital signature process verifies the sender to be authentic and the data valid. If these do not verify, then the document is flagged for manual intervention. If verified, then the data packet transported via the PDF can be used to verify that the variable and MICR data on the face of the document has not been altered and is indeed correct. The utilization of these three data sources (PDF, variable data, and MICR line) enables authentication of the document. The hash coding function verifies the time, content, point of origin, and originator of the symbol data in a manner which cannot be repudiated. When combined, these processes provide positive proof of the document's authenticity and validity. Thus, a system and method according to the invention seeks to be fraud proof, rather than fraud resistant.

DEPR: In step 430, the user account ID, document creation date, and some or all of the flags from step 420 are used to look up the public key(s) that should be employed to decrypt the data and verify the document . The document creation date is utilized to support periodically changing the key sets. Because of the lag in the paper processing system, it is possible that in the time between a creation of an item and the processing of that item, the key sets for a given customer/account have been changed. The inclusion of the document creation date insures that the proper set is used. The flags read in step 420 are needed so that the exact encryption algorithm used in the creation process can be determined and the proper key set returned.

CLPV: a printing unit communicatively coupled to the merge image and signature unit and configured to print a self -authenticating symbol onto the encrypted data output by the merge image and signature unit.